Flossbach von Storch
RESEARCH INSTITUTE

MAKRO 10/08/2023

"De-Risking" kritischer Infrastrukturen

AGNIESZKA GEHRINGER

Zusammenfassung

Mit der Verschärfung autoritärer Tendenzen, insbesondere in China, haben die geopolitischen Risiken zugenommen. Um diesen Risiken zu begegnen, ist ein umfassender und kohärenter Ansatz erforderlich. Insbesondere in der Europäischen Union ist ein aktiveres und systematischeres Vorgehen geboten, um das gemeinsame Verständnis für kritische Infrastrukturen und ihre sektoralen und grenzüberschreitenden Abhängigkeiten zu verbessern. Andernfalls würde das neue Mantra von der "De-Risking" der Beziehungen zu China zu einer leeren Phase werden.

Abstract

With intensifying authoritarian tendencies particularly in China, geopolitical risks have increased. A comprehensive and coherent framework is needed to address these risks. Especially in the European Union, a more active and systematic dialog is required to enhance the common understanding of critical infrastructures and their sectoral and transboundary interdependences. Failing to do so would turn the new mantra of “de-risking” relations with China into an empty phase.

1. Einführung

Aufgrund einer Reihe von makroökonomischen Risikoereignissen in jüngster Zeit ist die Besorgnis über kritische Infrastrukturen bei Regierungen und Experten weltweit gestiegen. Die Wahrnehmung dessen, was konkret als kritische Infrastrukturen gilt und welche Risiken damit verbunden sind, insbesondere wenn die Kontrolle über sie an ausländische Betreiber abgegeben wird, ist jedoch von Land zu Land sehr unterschiedlich. Dies könnte problematisch sein, da kritische Infrastrukturen durch starke grenzüberschreitende Interdependenzen gekennzeichnet sind und daher eine grenzüberschreitende Zusammenarbeit erfordern. Darüber hinaus können staatliche Strategien im Zusammenhang mit kritischen Infrastrukturen erhebliche geopolitische Auswirkungen haben. Diese Studie fasst die bestehenden Konzepte und Ansätze zur Identifizierung und zum Schutz kritischer Infrastrukturen zusammen und konzentriert sich dabei auf die wichtigsten Volkswirtschaften der entwickelten Welt.

2. Was ist eine kritische Infrastruktur?

Kritische Infrastruktur spielt eine zentrale Rolle für das wirtschaftliche und soziale Wohlergehen.

Trotz der großen Komplexität des Themas besteht in der wissenschaftlichen Gemeinschaft, unter Experten und politischen Entscheidungsträgern ein Konsens über die allgemeine Definition kritischer Infrastrukturen. Eine **kritische Infrastruktur** umfasst einzelne oder mehrere Anlagen oder Systeme – physisch, organisatorisch oder virtuell – die für die Gesellschaft so lebenswichtig sind, dass ein Ausfall oder eine Beeinträchtigung ihrer Leistung zu anhaltenden Versorgungsengpässen und/oder zu schwerwiegenden und unerwünschten Auswirkungen auf lebenswichtige gesellschaftliche Funktionen, einschließlich Gesundheit, Sicherheit, wirtschaftliches oder soziales Wohlergehen der Menschen, führen würde (OECD 2019, Alcaraz & Zeadally 2015). Dementsprechend liegt der Schwerpunkt auf der zentralen Rolle, die das Funktionieren von kritischen Infrastrukturen für das wirtschaftliche und soziale Wohlergehen spielt.[1]

In der Regel werden kritische Infrastrukturen im nationalen Kontext identifiziert, was zum Begriff der **nationalen kritischen Infrastruktur** führt. Im Kontext der EU werden zusätzlich **europäische kritische Infrastrukturen** genannt. Dabei handelt es sich um "die ausgewiesenen kritischen Infrastrukturen, die für die Gemeinschaft von größter Bedeutung sind und die bei einer Störung oder Zerstörung zwei oder mehr MS [Mitgliedstaaten] oder einen

[1] Es gibt einige andere - oft von der Regierung entwickelte - Definitionen, die die Bedeutung von kritischen Infrastrukturen für das Funktionieren des Staates oder die nationale Sicherheit betonen (OECD 2019). Zu den Beispielen hierfür gehören die ehemaligen kommunistischen Länder in Osteuropa, nämlich die Tschechische Republik, Lettland, die Slowakische Republik und Polen.

einzigen Mitgliedstaat beeinträchtigen würden, wenn sich die kritische Infrastruktur in einem anderen Mitgliedstaat befindet" (EC 2006, S. 4).[2]

Kritische Infrastrukturen sind durch vielfältige Interdependenzen gekennzeichnet.

Ein charakteristisches Merkmal kritischer Infrastrukturen sind die **gegenseitigen Abhängigkeiten** zwischen den einzelnen Infrastrukturen. Sie zeigen sich in sektorübergreifenden Abhängigkeiten bei der Beschaffung und Umsetzung von Produkten und Dienstleistungen, die von einer kritischen Infrastruktur bereitgestellt werden und für das reibungslose Funktionieren einer anderen kritischen Infrastruktur unerlässlich sind (Laugé *et al*. 2015). Darüber hinaus können Interdependenzen grenzüberschreitender Natur sein, wenn das Funktionieren einer kritischen Infrastruktur in einem Land von einer anderen kritischen Infrastruktur im Ausland abhängt.

Neben den sektoralen Merkmalen gibt es vier Ebenen von Interdependenzen zwischen kritischen Infrastrukturen (Rinaldi *et al*. 2001):

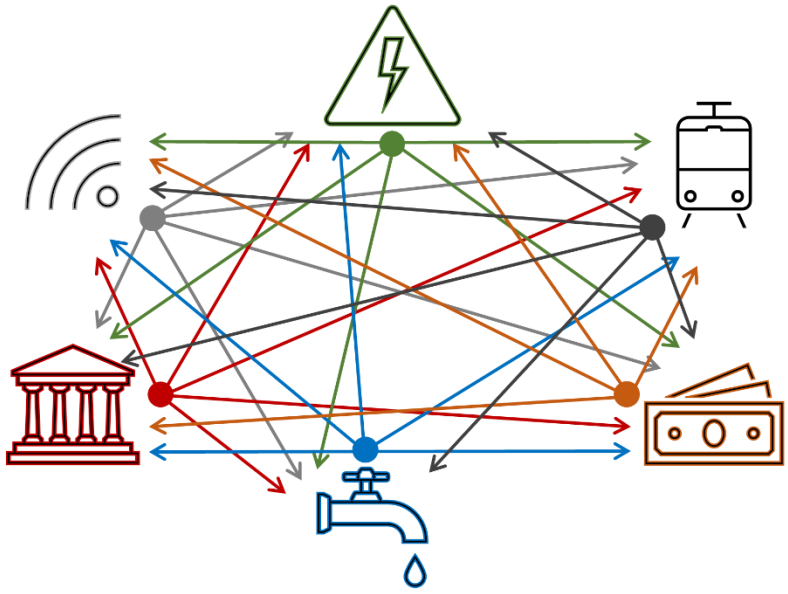
→ *physisch*: Der Betrieb der einen Infrastruktur hängt von der/den materiellen Leistung(en) der anderen ab;
→ *cyber*: Abhängigkeit von Informationen, die über die Informationsinfrastruktur übertragen werden;
→ *geografisch*: Abhängigkeit von lokalen Umwelteinflüssen, die gleichzeitig mehrere Infrastrukturen in einem bestimmten Gebiet betreffen;
→ *logisch*: jede Art von Abhängigkeitsmechanismus, der nicht der physischen, cyber oder geografischen Ebene zuzuschreiben ist, z. B. menschliche Entscheidungen und Handlungen.

Da es sich bei kritischen Infrastrukturen in der Regel um komplexe Systeme handelt, können mehrere Kombinationen der vier Dimensionen und somit mehrschichtige Interdependenzen zwischen jedem bilateralen Satz von kritischer Infrastruktur gleichzeitig auftreten. In **Abbildung 1** wird die zugrundeliegende Komplexität in einem vereinfachten Rahmen für die sechs kritischen Infrastrukturen Energie, Wasser, Verkehr, Information und Kommunikation,

[2] Die Richtlinie (EU) 2022/2557 ändert diesen Rahmen geringfügig ab. Insbesondere sollte jeder Mitgliedstaat auf der Grundlage der Liste der 11 Sektoren die kritischen Einrichtungen in diesen Sektoren bestimmen. Die Richtlinie definiert den Begriff "kritische Infrastruktur" als "einen Vermögenswert, eine Einrichtung, eine Ausrüstung, ein Netz oder ein System oder einen Teil eines Vermögenswertes, einer Einrichtung, einer Ausrüstung, eines Netzes oder eines Systems, der/die für die Erbringung eines wesentlichen Dienstes erforderlich ist", klärt aber nicht die begriffliche oder praktische Verbindung zur kritischen Einheit. Nach dem Wortlaut der Richtlinie sind kritische Einheiten jedoch Betreiber einer oder mehrerer kritischer Infrastrukturen (Art. 13(1b), Art. 21(1a)). Darüber hinaus bezieht sich die Richtlinie nicht ausdrücklich auf europäische kritische Infrastruktur, sondern verlangt eine Zusammenarbeit zwischen den Mitgliedstaaten für den Fall, dass ihre kritischen Einheiten "kritische Infrastrukturen nutzen, die physisch zwischen zwei oder mehreren Mitgliedstaaten verbunden sind" (Artikel 11 Absatz 1a). Schließlich werden in der Richtlinie kritische Einheiten von besonderer europäischer Bedeutung als Einheiten bezeichnet, die "dieselben oder ähnliche wesentliche Dienste für sechs oder mehr Mitgliedstaaten erbringen" (Artikel 17 Absatz 1b).

Finanzen und Staat aufgeschlüsselt. Jeder sektorale Knotenpunkt ist in beide Richtungen von jedem anderen sektoralen Knotenpunkt abhängig. Diese wechselseitigen Abhängigkeiten werden durch alle vorgenannten Ebenen kanalisiert. So ist beispielsweise der Bereich Information und Kommunikation ein wichtiger Lieferant sowohl von materiellen Leistungen (Netze, Hardware) als auch von Informationen (Telefon- und Mobilfunkdienste) für alle anderen kritischen Infrastrukturen. Darüber hinaus ist diese Vernetzung oft grenzüberschreitend - wenn beispielsweise Energieversorger aus verschiedenen Ländern relevante Informationen austauschen. Da menschliche Interaktionen ein unverzichtbarer Bestandteil dieser Kommunikation sind, ist auch die logische Ebene naturgemäß beteiligt.

Abbildung 1. Mehrdimensionale Interdependenzen zwischen kritischen Infrastrukturen



Quelle: Eigene Darstellung Flossbach von Storch Forschungsinstitut, basierend auf Rinaldi et al. (2001)

Dementsprechend müssen kritische Infrastrukturen in einem systemischen, sektorübergreifenden und mehrschichtigen Ansatz betrachtet werden, bei dem alle Arten direkter und indirekter, physischer, virtueller, geografischer und logischer Abhängigkeiten berücksichtigt werden. Schließlich bestehen die Abhängigkeiten nicht nur innerhalb nationaler Grenzen, sondern können auch eine starke internationale Dimension haben. Daraus folgt, dass Bedrohungen nicht in einem rein nationalen Kontext bewertet werden können. Die Verflechtung der heutigen Wirtschaft - z. B. ICT-Systeme und Finanzinfrastrukturen - und Gesellschaft bedeutet, dass externe Störungen schwerwiegende Auswirkungen auf die inländischen kritischen Infrastrukturen haben können – und vice versa.

Während die Anerkennung und Konzeptualisierung von Interdependenzen, Verflechtungen und der grenzüberschreitenden Dimension in Fachkreisen

weit fortgeschritten und allgemein bekannt sind, haben sie sich in der praktischen Anwendung in den Ländern und Regionen bisher weit weniger niedergeschlagen (OECD 2019).

3. Wie werden kritische Infrastrukturen klassifiziert?

Tabelle 1 gibt einen Überblick über die bestehenden sektoralen Klassifikationen in den wichtigsten Industrieländern. Die US-Klassifizierung wird als Referenz für die sektoralen Bezeichnungen herangezogen, da die USA über den am weitesten entwickelten und umfassendsten Handlungsrahmen für kritische Infrastrukturen und deren Schutz verfügen.

Die US-Klassifikation ist nicht immer vollkommen kompatibel mit anderen Klassifikationen, und die sektoralen Bezeichnungen unterscheiden sich manchmal. So werden beispielsweise in der US-Klassifikation Kommunikations- und Informationstechnologie getrennt behandelt, während in Deutschland, Kanada und Japan diese beiden Sektoren gemeinsam als Informations- und Kommunikationstechnologien betrachtet werden.

Energie, Verkehr, Kommunikation, Informationstechnologie, Lebensmittel, Gesundheit, Wasser, Finanzen und Regierung gehören zu den Kernbereichen von kritischen Infrastrukturen.

Trotz dieser Unterschiede besteht zumindest ein Konsens über die Kerngruppe der Sektoren/Aktivitäten, die als kritische Infrastruktur bezeichnet werden. In allen Klassifizierungen gehören Energie, Verkehr, Kommunikation, Informationstechnologie, Nahrungsmittel, Gesundheit, Wasser, Finanzen und Regierungsdienste fast eindeutig zu den kritischen Infrastrukturen. Andere Sektoren sind eher länderspezifisch. Dies betrifft so scheinbar wichtige Sektoren wie Verteidigung, Chemie, kommerzielle Einrichtungen, kritische Produktion, Staudämme, Notdienste und den Nuklearsektor.

In einigen Ländern wird bei der Klassifizierung von Sektoren mit kritischen Infrastrukturen die Hauptverantwortung einer bestimmten Behörde oder eines Ministeriums zugewiesen. In den USA beispielsweise fällt jeder Sektor in den Zuständigkeitsbereich einer bestimmten sektorspezifischen Agentur (*Sector-Specific Agency*, SSA), bei der es sich um ein Bundesministerium oder eine andere Regierungsstelle handelt. Die wichtigste Einrichtung in diesem Sinne ist das Ministerium für Heimatschutz (*Department of Homeland Security*), das für 10 von 16 kritischen Infrastrukturen zuständig ist. In der EU verlangt die jüngste Richtlinie (EU) 2022/2557 von den Mitgliedstaaten die Benennung von Behörden, die für die ordnungsgemäße Anwendung und Durchsetzung der in der Richtlinie festgelegten Vorschriften zuständig sind, sowie von einheitlichen Ansprechpartnern, die die grenzüberschreitende Zusammenarbeit gewährleisten.

Tabelle 1. Überblick über die bestehenden Klassifizierungen kritischer Infrastrukturen in den wichtigsten Volkswirtschaften weltweit

Kritische Infrastrukturen	USA	EU	Deutsch-land	Frank-reich	Kanada	UK	Austral-ien	Japan
Chemie	+					+		+
Kommerzielle Einrichtungen	+							+[5]
Kommunikation	+	+[1]	+[2]	+	+[2]	+	+	+[2]
Kritische Industrie	+			+[4]	+			
Staudämme	+							
Notfalldienste	+				+	+		
Staatliche Einrichtungen	+	+	+	+	+	+		+
Informationstechnologie	+	+[1]	+[2]	+	+[2]		+[3]	+[2]
Kernreaktoren, Materialien und Abfälle	+					+		
Transportsysteme	+	+	+	+	+	+	+	+
Verteidigungsindustrie	+			+		+	+	
Energie	+	+	+	+	+	+	+	+[6]
Finanzdienstleistungen	+	(+)	+	+	+	+	+	+
Lebensmittel und Landwirtschaft	+	(+)	+	+	+	+	+	
Gesundheitswesen und öffentliche Gesundheit	+	(+)	+	+	+	+	+	+
Wasser- und Abwassersysteme	+	(+)	+	+	+	+	+	+
Katastrophenschutz und -management			+					
Nationale Denkmäler und Ikonen			+					
Medien			+					
Weltraum		(+)		+		+	+	
Hochschulbildung und Forschung				+			+	

Quelle: USA - National Infrastructure Protection Plan 2013; EU - Richtlinie 2008/114/EG des Rates, Einträge in Klammern beziehen sich auf Sektoren, die mit der Richtlinie (EU) 2022/2557 hinzugefügt wurden, die die Richtlinie 2008/114/EG des Rates ab dem 18. Oktober 2024 aufheben wird; Deutschland - FMI (2009); Frankreich - Arrêté du 3 juillet 2008 portant modification de l'arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desditssecteurs; Kanada - National Strategy for Critical Infrastructure of 2010; Vereinigtes Königreich - Public Summary of Sector Security and Resilience Plans of 2018; Australien - Security of Critical Infrastructure Act 2018; Japan - Fourth Action Plan for Information Security of Critical Infrastructure（重要インフラの情報セキュリティ対策に係る第４次行動計画（改定)).

[1] Der Sektor wird als "digitale Infrastruktur" bezeichnet. [2] Es wird gemeinsam auf die Informations- und Kommunikationstechnologien Bezug genommen. [3] Der Sektor wird als "Datenspeicherung und -verarbeitung" bezeichnet. [4] Der Sektor wird als "Industrie" bezeichnet. [5] Der Sektor wird als "Logistikdienstleistungen" bezeichnet. [6] Die Klassifizierung unterscheidet zwischen drei energiebezogenen Sektoren, nämlich "Stromversorgungsdienste", "Gasversorgungsdienste" und "Erdölindustrie".

Auch Australien hat einen transparenten und detaillierten Rahmen für den Umgang mit kritischen Infrastrukturen entwickelt. Das Land führt nicht nur eine Liste von 11 kritischen Infrastruktursektoren auf, sondern auch eine umfangreiche Liste von 22 kritischen Infrastrukturanlagen als Teil der Sektoren, die als kritische Infrastruktur gelten. Diese Praxis ist in den anderen untersuchten Ländern nicht üblich.

Bis vor kurzem gab es in der EU keine genaue Klassifizierung kritischer Infrastrukturen.[3] Die einzige Bezugnahme auf konkrete Sektoren erfolgte in der Richtlinie 2008/114/EG des Rates, wobei der Schwerpunkt auf Energie und Verkehr lag und der Informations- und Kommunikationstechnologiesektor in den nachfolgenden Schritten analysiert und überprüft werden sollte. Mit der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates wurde eine Klassifizierung mit 11 Sektoren – wie in **Tabelle 1** aufgeführt – erarbeitet. Die Richtlinie (EU) 2022/2557 wird die Richtlinie 2008/114/EG des Rates ab dem 18. Oktober 2024 aufheben. Eine wichtige Herausforderung innerhalb der EU für eine funktionierende Koordinierung und einen wirksamen Schutz kritischer Infrastrukturen besteht darin, dass sich die Länder bei der Definition, Identifizierung und Verwaltung kritischer Infrastrukturen stark unterscheiden. Ein extremes Beispiel ist Italien, wo es weder eine Strategie bzgl. der kritischen Infrastrukturen noch eine federführende Institution für kritische Infrastrukturen gibt (OECD 2019). Auch Portugal beschränkt seine Politik in Bezug auf kritische Infrastruktur auf zwei Sektoren – Energie und Verkehr – wie in der Richtlinie 2008/114/EG des Rates festgelegt.

Aufgrund der grenzüberschreitenden Interdependenzen zwischen kritischen Infrastrukturen und der daraus resultierenden Notwendigkeit einer grenzüberschreitenden Zusammenarbeit sind Bemühungen um eine bessere Abstimmung und Harmonisierung der Vorgehensweisen in den einzelnen Ländern unabdingbar.

Diese unterschiedlichen Klassifizierungen und Unzulänglichkeiten in den zugrunde liegenden Strategien spiegeln häufig nationale Präferenzen und spezifische Prioritätenwahrnehmungen oder sogar ihr Fehlen wider. Aufgrund der grenzüberschreitenden Interdependenzen zwischen kritischen Infrastrukturen und der daraus resultierenden Notwendigkeit einer grenzüberschreitenden Zusammenarbeit sind Bemühungen um eine bessere Abstimmung und Harmonisierung der Ansätze in den einzelnen Ländern jedoch eine unverzichtbare Risikomanagementstrategie.

4. Die blinden Flecken in der jüngsten Politik zum Schutz von kritischer Infrastruktur

Bei den bisherigen Erfahrungen mit dem Schutz von kritischen Infrastrukturen lassen sich zwei Hauptprobleme identifizieren. Erstens führt die

[3] Tatsächlich hat die Europäische Kommission im Jahr 2005 ein Grünbuch über ein Europäisches Programm für den Schutz kritischer Infrastrukturen mit einer indikativen und detaillierten Liste von 11 kritischen Infrastruktursektoren veröffentlicht (EC 2005). Diese Klassifizierung wurde jedoch in den nachfolgenden offiziellen Dokumenten zu diesem Thema nicht mehr berücksichtigt.

Vernachlässigung der grenzüberschreitenden Interdependenzen zwischen kritischen Infrastrukturen zu einer **schwachen Zusammenarbeit** bei der Schaffung eines robusten Rahmens für das Risikomanagement von kritischen Infrastrukturen. Zweitens waren die industriepolitischen Strategien der großen Industrieländer bisher oft unaufmerksam, wenn es darum ging, die **geopolitischen Auswirkungen** von Handels- und grenzüberschreitenden Investitionsstrategien zu berücksichtigen, die kritische Infrastrukturen im Inland betreffen.

Was die Zusammenarbeit anbelangt, so sind die bisherigen Strategien fragmentiert und beschränken sich auf lokalisierte zwischenstaatliche Initiativen. Die am stärksten institutionalisierte Initiative ist die der *Critical Five*, die 2012 von fünf Industrieländern - Australien, Kanada, Neuseeland, dem Vereinigten Königreich und den USA - gegründet wurde. Ziel der Initiative war es, den Informationsaustausch und die Arbeit an Themen von gemeinsamem Interesse zu verbessern. Die bisherigen Bemühungen waren konzeptioneller Art und zielten darauf ab, ein gemeinsames Verständnis von kritischen Infrastrukturen (Critical Five 2014) und von den Zusammenhängen zwischen Infrastrukturinvestitionen, Wirtschaftswachstum und Wohlstand im Rahmen der Critical-Five-Initiative zu finden (Critical Five 2015).

Innerhalb der EU wurden Anstrengungen unternommen, um sowohl die interne als auch die externe Zusammenarbeit zu stärken. Ein vielversprechender Schritt zur Förderung der internen Zusammenarbeit ist die Richtlinie (EU) 2022/2557, die ab dem 18. Oktober 2024 den entsprechenden Rahmen bilden wird. Aufgrund der bisherigen Erfahrungen mit der Verabschiedung der Vorgängerrichtlinie 2008/114/EG können jedoch Schwierigkeiten bei der Etablierung einer effektiven Kooperationspraxis nicht ausgeschlossen werden. Diese Annahme ist insofern realistisch, als die letztendliche Verantwortung für die nationale Sicherheit in den Händen der einzelnen Mitgliedstaaten und nicht auf EU-Ebene liegt und die Anreize zur Zusammenarbeit oft begrenzt waren. Was die externe Zusammenarbeit betrifft, so wurden Nachbarländer der EU und Länder des Europäischen Wirtschaftsraums (Norwegen, Island und Liechtenstein) sowie andere Länder in Europa und darüber hinaus einbezogen. Bei den meisten Initiativen handelte es sich jedoch um eine rein informelle Zusammenarbeit, um Workshops und Expertentreffen mit einem vage definierten Austausch bewährter Verfahren, sowie um Bemühungen – von Deutschland mit Russland – die offensichtlich aufgrund einer Fehleinschätzung der Risiken im Zusammenhang mit der Verfolgung imperialistischer Ambitionen gescheitert sind. Eine Ausnahme bildet die Zusammenarbeit innerhalb der NATO, die kürzlich zu einer detaillierten Untersuchung der aktuellen Sicherheitsherausforderungen bei kritischen Infrastrukturen in den Bereichen Energie, Verkehr, digitale Infrastruktur und Weltraum geführt hat (EU/NATO 2023). Nichtsdestotrotz fehlt es noch immer an einem

weitreichenderen und ergebnisorientierten Instrumentarium für die Zusammenarbeit (Lazari & Mikac 2022).

Die fehlende Sensibilität für geopolitische Fragen beim Schutz von kritischen Infrastrukturen lässt sich auf die früheren industriepolitischen Strategien zurückführen, die im globalen Rahmen der Liberalisierung der grenzüberschreitenden Waren-, Dienstleistungs- und Produktionsströme, einschließlich technologischen Know-hows und Informationen, durchgeführt wurden. Das vorherrschende Paradigma freier Märkte und offener Volkswirtschaften wurde bedingungslos auf eine breite Palette von Sektoren angewandt, unabhängig von ihrem Status als kritische Infrastruktur. Dies führte häufig zum Erwerb von Vermögenswerten aus dem Ausland auch in Sektoren, die als kritische Infrastruktur gelten, wobei es mitunter zu erheblichen Eigentumsverlagerungen ins Ausland kam. Dieser Prozess vollzog sich weitgehend in der EU, aber auch in anderen entwickelten Volkswirtschaften, darunter den USA.

Unter den großen Erwerbern waren chinesische Investoren intensiv an der Übernahme von Betreibern kritischer Infrastrukturen beteiligt. Auf sektoraler Ebene investierte China weltweit stark in die Hafeninfrastruktur, und wichtige europäische Hafenterminals befinden sich heute teilweise oder vollständig im Besitz chinesischer Betreiber (Jüris 2023, Geinitz 2022). Auch die chinesischen Investitionen in die US-amerikanischen Kommunikations- und Informationstechnologien schritten in den 1990er und 2000er Jahren unaufhaltsam voran (Hillman 2021). Schließlich erobert sich China eine Nische als bevorzugter Anbieter von Informations- und Kommunikationsinfrastrukturen für Entwicklungsländer. Peking intensiviert derzeit seine Bemühungen um den Verkauf von Kommunikationssatelliten im globalen Süden. Der chinesische Digitalriese Huawei ist derzeit in mehr als 170 Ländern aktiv. Zwei weitere chinesische Technologieunternehmen, Hikvision und Dahua, liefern rund 40 % der Überwachungskameras weltweit. Schließlich gehört die Hengtong-Gruppe zu den vier wichtigsten globalen Anbietern von Unterseekabeln, über die mehr als 95 % des internationalen Datenverkehrs abgewickelt werden (Hillman 2021).

Dieser Prozess der Intensivierung von ausländischen Direktinvestitionen und Handelsbeziehungen wurde lange Zeit als integraler Bestandteil der Demokratisierung nicht-demokratischer Länder angesehen, die ideologisch durch den Wandel durch Handel sowie durch die befreiende Wirkung von Kommunikationstechnologien und des offenen Cyberspace motiviert war (Gehringer 2023, Hillman 2021). Mit der Verschärfung der autoritären Tendenzen, die insbesondere in Chinas Regierungsstil unter Xi Jinping zum Ausdruck kommen, werden die geopolitischen Risiken für Länder, die ihre Kontrolle über kritische Infrastrukturen an chinesische Unternehmen abgeben, jedoch nicht unerheblich. Dies ist darauf zurückzuführen, dass Chinas zentralisiertes und

parteigeführtes politisches System die Unterscheidung zwischen wirtschaftlichen, politischen und militärischen Interessen verwischt (Jüris 2023, Cristiani *et al*. 2021). Die autoritäre Führung der Kommunistischen Partei Chinas (KPCh) sieht die Angleichung der Interessen des Staates und privater Unternehmen explizit als eine zentrale Strategie zur Erreichung nationaler strategischer Ziele an. Letztere betreffen naturgemäß industriepolitische Ziele im Inland, gehen aber oft auch über die Landesgrenzen Chinas hinaus (Gehringer 2023).[4] So tragen international ausgerichtete chinesische Unternehmen dazu bei, den Einfluss der KPCh im Ausland auszuweiten und - genauer gesagt - die Volksbefreiungsarmee durch Technologietransfer zu modernisieren (Jüris 2023, Hillman 2021). Diese Strategie ist insofern durchsetzbar, als sich zahlreiche Unternehmen in China in Staatsbesitz befinden oder - wenn sie vermeintlich privat sind - unter starkem Einfluss der KPCh stehen, und zwar über die KPCh-nahen Managementmitglieder. Zudem werden international tätige Unternehmen häufig finanziell incentiviert und operativ unterstützt, um zur Erreichung der strategischen Ziele Chinas beizutragen.

Mit der zunehmenden Erkenntnis der Risiken, die mit der bedingungslosen Liberalisierung der grenzüberschreitenden Wirtschaftsbeziehungen verbunden sind, haben die Regierungen, vor allem in den Industrieländern, begonnen, ihre Industriepolitik zu überdenken und einen Ansatz zur Risikominderung zu verfolgen, insbesondere wenn kritische Infrastrukturen und Einrichtungen betroffen sind.

Zu den ersten Akteuren in dieser Hinsicht gehörte Washington, wo Geheimdienstbeamte in einem Kongressbericht aus dem Jahr 2012 davor warnten, dass die chinesische Technologie-Infrastruktur die US-Netzwerke gefährden könnte.[5] Im Jahr 2019 verbot die Federal Communication Commission den Kauf von Geräten von Huawei und ZTE.[6] Die Warnungen der USA vor den oben genannten Risiken werden inzwischen auch von anderen Regierungen in Australien, Japan und Westeuropa wahrgenommen.

Trotz einer erheblichen Verzögerung hat die EU kürzlich ihre Strategie gegenüber China überdacht. In der gemeinsamen Mitteilung "Strategischer

[4] Solche Ziele wurden in verschiedenen strategischen KPCh-Dokumenten und nationalen Programmen formuliert, wie z. B. der Gürtel- und Straßeninitiative (BRI), Made in China 2025, China Standards 2035 oder Chinas Militär-Zivil-Fusionsstrategie.

[5] "Untersuchungsbericht über die Probleme der nationalen Sicherheit der USA, die von den chinesischen Telekommunikationsunternehmen Huawei und ZTE ausgehen. U.S. House of Representatives. Verfügbar unter: https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf.

[6] "Schutz vor nationalen Sicherheitsbedrohungen für die Kommunikationslieferkette durch FCC-Programme". Federal Communications Commission. Verfügbar unter: https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

Ausblick" vom März 2019 erklärte die EU, dass sie China weiterhin gleichzeitig als Kooperations- und Verhandlungspartner, als wirtschaftlichen Konkurrenten beim Streben nach technologischer Führerschaft und als systemischen Konkurrenten bei der Förderung alternativer Governance-Modelle behandeln will (EC 2019). Darüber hinaus hat die EU im Rahmen der grenzüberschreitenden Beziehungen unerwünschten Transaktionen und Investitionspraktiken einen Riegel vorgeschoben. Im Frühjahr 2019 verabschiedete die Gemeinschaft eine Verordnung zur Schaffung eines neuen EU-weiten Rahmens für die Überprüfung von ausländischen Direktinvestitionen. Obwohl die Verordnung als lockeres Koordinierungs- und Kooperationsinstrument kritisiert wird, bei dem die EU-Mitgliedstaaten relevante Informationen über einzelne Auslandsinvestitionen austauschen können, die sich auf ihre nationale Sicherheit und öffentliche Ordnung auswirken könnten, stellt sie einen entscheidenden Schritt dar, um das Bewusstsein zu schärfen und die Konvergenz der verstreuten nationalen FDI-Strategien zu fördern (Hanemann *et al*. 2019). Darüber hinaus sind ähnliche Maßnahmen erforderlich, um andere Formen der direkten und indirekten Beteiligung ausländischer Akteure an kritischen Infrastrukturen zu prüfen.

5. Fazit

Ausländisches Eigentum an inländischen kritischen Infrastrukturen kann unerwünschte Folgen für die nationale Sicherheit und die öffentliche Ordnung haben. Insbesondere Chinas Einfluss auf kritische Infrastrukturen in den Industrieländern stellt ein ernstes Risiko für die strategische Souveränität der beteiligten Länder dar. Die Entschlossenheit der KPCh, strategische nationale Ziele zu erreichen, setzt häufig das direkte Engagement und den Beitrag chinesischer, KPCh-treuer Einrichtungen im In- und Ausland voraus.

Sicherheitslücken im Schutz von kritischen Infrastrukturen führen zur weiteren Ausbreitung unerwünschter Einflüsse aus China und allgemeiner nicht-demokratischer Systeme.

Das Engagement Chinas in kritischen Infrastrukturen im Ausland begann in einem regulatorischen und politischen Vakuum, bevor die Regierungen der führenden Industrieländer begannen, Bedenken hinsichtlich nationaler Sicherheitsfragen zu äußern. Obwohl einige Gegenmaßnahmen ergriffen und Strategien zum Schutz kritischer Infrastrukturen entwickelt wurden, ist der daraus resultierende Rahmen noch immer unterentwickelt und fragmentiert. Infolgedessen führen Sicherheitslücken zu einer weiteren Ausbreitung unerwünschter Einflüsse aus China und allgemeiner aus nicht-demokratischen Systemen.

Zur Bewältigung dieser Risiken ist ein umfassender und kohärenter Rahmen erforderlich. Was speziell die EU betrifft, so ist ein aktiverer und systematischerer Dialog erforderlich, um das gemeinsame Verständnis kritischer Infrastrukturen und ihrer sektoralen und grenzüberschreitenden Interdependenzen zu verbessern. Dadurch sollte ein Rahmen für einen regelmäßigen

Austausch relevanter Erkenntnisse geschaffen werden, insbesondere in Bezug auf die Eigentumsstruktur und andere Formen risikoreicher ausländischer Beteiligungen am Betrieb kritischer Infrastrukturen. Ein einheitliches EU-Konzept für kritische Infrastrukturen mag schwierig zu erreichen sein, ist aber ein sicherer Schutz gegen nachteilige strategische Rivalitäten.

Literatur:

Critical Five (2015). Role of critical infrastructure in national prosperity. Available at: https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-ci-national-prosperity-2015-508.pdf.

Critical Five (2014). Forging a common understanding for critical infrastructure. Available at: https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf.

EC (European Commission) (2019). Joint Communication to the European Parliament, the European Council and the Council: EU-China – A strategic outlook. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0005.

EC (European Commission) (2006). Communicaton from the Commission on a European Programme for Critical Infrastructure Protection, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

EC (European Commission) (2005). Green paper on a European Programme for Critical Infrastructure Protection, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576

EU/NATO (2023). EU-NATO task force on the resilience of critical infrastructure. Final Assessment Report. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/EU-NATO_Final_Assessment_Report_Digital.pdf.

European Council (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union, L 345/75, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

FMI (Federal Ministry of the Interrior of Germany) (2009). National strategy for critical infrastructure protection (CIP strategy), available at: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=2.

Geinitz, C. (2022). Chinas Greif nach dem Westen. Wie sich Peking in unsere Wirtschaft einkauft. C.H. Beck: München.

Gehringer, A. (2023). Calibrating the EU's trade dependence. *Survival* 65(1), 81-96.

Hanemann, T., Huotari, M., Kratz, A. (2019). Chinese FDI in Europe: 2018 trends and impact of new screening policies. Rhodium Group and the Mercator Institute for China Studies (MERICS).

Hillman, J.E. (2021). Chinas digitale Seidenstrasse. Der globale Kamp um die Herrschaft über die Daten. Plassen Verlag: Kulmbach.

Jüris, F. (2023). Security implications of China-owned critical infrastructure in the European Union. European Parliament, Directorate-General for External Policies. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf.

Laugé, A. Hernantes, J. Sarriegi, J. (2013). Disasterimpact assessment: aholisticframework. In: Proceedings of the Tenth International Conference on Information Systems for Crisis Response and Management, pp. 730–734.

Lazari, A., Mikac, R. (2022). The External Dimension of the European Union's Critical Infrastructure Protection Programme: From Neighbouring Frameworks to Transatlantic Cooperation. CRC Press.

OECD (2019). Good Governance for Critical Infrastructure Resilience. OECD Publishing, Paris.

Cristiani, D., Ohlberg, M., Parello-Plesner, J., Small, A. (2021). The security implications of Chinese infrastructure investment in Europe. The German Marshall Fund of the United States. Available at: https://www.gmfus.org/sites/default/files/2022-01/Cristiani%20et%20al%20-%20report%20(1)%20Updated.pdf.

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, p. 11-25.

RECHTLICHER HINWEIS

STANDORTINFORMATIONEN

Herausgeber: Flossbach von Storch AG, Forschungsinstitut, Ottoplatz 1, 50679 Köln, Deutschland; Telefon +49 221 33 88-291, research@fvsag.com Geschäftsführer: Dr. Bert Flossbach, Kurt von Storch, Dirk von Velsen; *Eintragung*: Nr. 30 768 im Handels- und Firmenregister beim Amtsgericht Köln; *USt.-Nr.* DE200075205; **Aufsichtsbehörde**: Bundesanstalt für Finanzdienstleistungsaufsicht, Marie-Curie-Straße 24 - 28, 60439 Frankfurt / Graurheindorfer Straße 108, 53117 Bonn, www.bafin.de; *Autor*: Prof. Dr. Agnieszka Gehringer; *Redaktionsschluss:* 09. August 2023